AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the
Central District of California

UNITED STATES OF AMERICA,

v.

SHIRZAD MEHRRAFIEE,

Defendant.

Case No. 2:25-mj-00593-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date of June 27, 2020, in the County of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1349	Conspiracy to commit wire fraud

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Special Agent Michael Ruccia, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: February 9, 2025

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenbluth, U.S.M.J.
Printed name and title

AUSA: Kedar S. Bhatia (x4442)

AFFIDAVIT

I, Michael Ruccia, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. This affidavit is made in support of a criminal complaint and arrest warrant against Shirzad MEHRRAFIEE for a violation of 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud).

2. This affidavit is also made in support of search warrants for the following:

a. The property located at 6345 Balboa Boulevard, Building 3, #257, Encino, California 91316 ("SUBJECT PREMISES-1"), as further described in Attachment A-1;

b. The property located at 84 Stagecoach Road, Bell Canyon, California 91307 ("SUBJECT PREMISES-2"), as further described in Attachment A-2;

c. The white Mercedes Maybach, California license plate 9LCT781 and Vehicle Identification Number ("VIN") W1K6X7KB3RA258152 (the "SUBJECT VEHICLE"), as further described in Attachment A-3; and

d. The person of Shirzad MEHRRAFIEE, as further described in Attachment A-4.

3. The items to be seized are described in Attachment B, which are the evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud); 18 U.S.C. § 1956 (Money Laundering); 18 U.S.C. § 1957 (Transacting in Criminal Proceeds Over $10,000); 18 U.S.C. § 1956(h) (Conspiracy to Commit Money

Laundering); 18 U.S.C. § 1960 (Unlicensed Money Transmitting Business); 15 U.S.C. § 645 (False Statements to the SBA); and 18 U.S.C. § 371 (Conspiracy to Make False Statements to the SBA) (the "Subject Offenses"). Attachments A-1, A-2, A-3, A-4, and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based on my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses, including my review of reports prepared by other law enforcement officers and agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of the investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF THE AFFIANT

5. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since April 2022. I am currently assigned to the Los Angeles Field Office, Ventura Resident Agency of the FBI. I am a federal agent empowered by the United States law to conduct investigations of, and make arrests for, offenses enumerated in Title 18 of the United States Code. Since 2022, I have been assigned to a counterintelligence squad where my primary responsibility is the investigation of matters involving foreign counterintelligence and counterproliferation. I have completed FBI training in

foreign counterintelligence matters, which has included training in criminal violations associated with espionage, economic espionage, money laundering, and counterproliferation. In the course of my career, I have participated in the service of multiple federal search warrants relating to counterintelligence investigations.

III. SUMMARY OF PROBABLE CAUSE

6. As set forth below, there is evidence showing Shirzad MEHRRAFIEE has conducted a number of fraud schemes over the past five years that have left victims with millions of dollars in loss. *First*, in 2020 and 2021, MEHRRAFIEE and his co-conspirators submitted at least 17 applications to the SBA's Economic Injury Disaster Loan program using the names and identifying information for other people. As a result of the 17 fraudulent applications, the SBA paid out more than $2.6 million in disaster loans that were never repaid. Approximately half of the money was transferred into bank accounts that MEHRRAFIEE solely controlled. The other half of the money went to various destinations, like luxury goods, stock brokerages, and cryptocurrency trading accounts. As discussed below, text message records obtained pursuant to a search warrant show MEHRRAFIEE texting with co-conspirators about the fraudulent applications, the stolen aliases, and the money disbursed by the SBA.

7. *Second*, in 2020, MEHRRAFIEE applied for an EIDL loan for one of the businesses he purportedly operates; however, he falsely stated in the application that he had never been

convicted of a felony crime. In fact, he has a prior federal felony conviction for presenting fake documents to a bank in order to secure a loan. He was sentenced to two years' imprisonment as a result of his prior federal conviction.

8. *Third*, in 2021, MEHRRAFIEE applied for and received a home mortgage loan worth approximately $3 million to purchase SUBJECT PREMISES-2. However, he inflated his monthly income, and his claim on the mortgage form is contradicted by tax records. In addition, MEHRRAFIEE submitted a false bank statement that grossly inflated his assets.

9. *Fourth*, in October 2024, MEHRRAFIEE and another individual who lives with him conducted a suspected kiting scheme at East West Bank. The scheme involved the two conspirators sending large wire transfers worth hundreds of thousands of dollars back-and-forth between accounts at two banks. As a result of the scheme, East West Bank lost a total of approximately $1.5 million.

10. *Finally*, between 2020 and 2024, MEHRRAFIEE deposited approximately $48 million – mostly in cash – into a handful of business bank accounts he controlled. Law enforcement officers doing surveillance on MEHRRAFIEE have seen him meeting with different individuals at gas stations and elsewhere to pick up bags, which he then took to banks to deposit money. One frequent contact, who recently delivered approximately $380,000 to MEHRRAFIEE, was arrested and charged this week for a conspiracy to launder $150,000 from the victim of an investment fraud scheme. One day after the arrest, the FBI learned that

MEHRRAFIEE, an Iranian citizen, had booked travel on February 9, 2025, to go from Los Angeles to Dubai and Dubai to Tehran, Iran. MEHRRAFIEE's flight from LAX is scheduled to leave at approximately 3:35 p.m. this afternoon.

IV. STATEMENT OF PROBABLE CAUSE

A. Background on the SBA and the EIDL Program

11. Based on my review of publicly available information, I have learned the following:

a. The SBA is an executive-branch agency of the United Stated government that provides support to entrepreneurs and small businesses. The mission of the SBA is to maintain and strengthen the nation's economy by enabling the establishment and viability of small businesses and by assisting in the economic recovery of communities after disasters. As part of this effort, the SBA facilitates loans through banks, credit unions, and other lenders. These loans have government-backed guarantees.

b. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act was a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans who were suffering the economic effects caused by the COVID-19 pandemic.

c. One source of relief provided by the CARES Act was the expansion of the COVID-19 EIDL Program. The EIDL Program was an SBA program designed to provide economic relief to eligible small businesses that were experiencing substantial financial disruption due to the COVID-19 pandemic. Through the

EIDL Program, the CARES Act authorized the SBA to provide working capital in the form of low interest, long-term loans. In addition, the CARES Act authorized the SBA to issue advances of up to $10,000 to small businesses applying for an EIDL. The advances did not have to be repaid.

d. To obtain an EIDL and advance, a qualifying business was required to submit an application to the SBA and provide information about its operations, such as the number of employees and the gross revenues for the 12-month period preceding the date of the disaster, designated as January 31, 2019, to January 31, 2020.

e. Applications were also required to answer whether they had any criminal history. Specifically, the application asked "for any criminal offense - other than a minor vehicle violation - have you ever been convicted, plead guilty, plead nolo contendere, been placed on pretrial diversion, or been placed on any form of parole or probation (including probation before judgment)?" (the "Criminal History Question").

f. Applicants certified that all the information in the application was true and correct to the best of their knowledge.

g. EIDL applications were submitted directly to the SBA. The amount of the loan was determined, in part, on the information provided by the applicant, including information about gross revenues.

h. Any funds issued under an EIDL or an advance were issued directly from the United States Treasury. EIDL funds

could be used for working capital to pay fixed debts, payroll, accounts payable, and other necessary business obligations that could not be met as a direct result of the COVID-19 disaster.

B. MEHRRAFIEE's Criminal History

12. Based on my review of court records and FBI records, I have learned the following:

a. In 2006, MEHRRAFIEE and two family members were charged in the U.S. District Court for the Western District of Missouri with one count one of conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349, and nine counts of bank fraud, in violation of 18 U.S.C. § 1344. *See* Indictment, *United States v. Mehrrafiee et al.*, No. 06-cr-310-W-SOW (W.D. Mo.), Dkt. 1.[1] MEHRRAFIEE was charged for a scheme to fraudulently obtain a series of bank loans by submitting vehicle titles with false information, creating and submitting false tax documents, and obtaining multiple loans based on the same collateral without disclosing prior loans to the banks. *See id.*

b. In 2007, MEHRRAFIEE pleaded guilty to one count of conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349. On November 14, 2007, the Hon. Scott O. Wright, United States District Judge, sentenced MEHRRAFIEE to 24 months imprisonment, five years of supervised release, and restitution of $523,132.72. In 2011, after MEHRRAFIEE violated certain terms of supervised release, the District Court continued him on supervised release with modified terms.

[1] Court records list several "also known as" names for MEHRRAFIEE: Rafie Mehrrafiee, Rocky Mehrrafiee, Rocky Rafie, and Shirzad Rafiee.

C. MEHRRAFIEE Scheme to Submit 17 Fraudulent EIDL Applications Causing $2.6 Million in Loss to the SBA

13. As set forth below, MEHRRAFIEE was responsible for submitting at least 17 different EIDL applications in the name of different individuals who were not present in the United States when the applications were submitted (the "17 Alias EIDL Applications"). Moreover, the bank accounts listed names that did not match driver's license records. SBA and bank records show the SBA disbursed approximately $2.6 million in loan funds as a result of the fraudulent loan applications. Approximately half of that money went into a small number of bank accounts for which MEHRRAFIEE was the lone authorized signer. The other half of the money went to other expenses. Text message records show MEHRRAFIEE talking with co-conspirators about the aliases and the money disbursed by the SBA.

14. Based on my review of SBA records, Wells Fargo Bank records, travel records, and driver's license records, I have learned the following:

a. Based on my review of the 17 Alias EIDL Applications, I have learned that each EIDL application was submitted in or around June 2020 or July 2020. In each application, the purported applicant provided a name, date of birth, social security number, and other identifiers.

b. In each application, the applicant stated that they operated a sole-proprietorship with the owner and applicant address that was located in the United States, frequently in the Southern California area or in Missouri, where MEHRRAFIEE

previously resided. As set forth above, MEHRRAFIEE's prior criminal case was in the U.S. District Court for the Western District of Missouri.

c. The 17 Alias EIDL Applications also listed a bank account into which the loan money, if granted, could be sent.

d. SBA records show that each of the 17 Alias EIDL Applications was funded. In some instances, the SBA also issued an EIDL advance, which was a loan amount up to $10,000 that was paid to the applicant soon after the application was filed, if they qualified.

e. None of the 17 Alias EIDL Applications has been repaid to the SBA, nor have any payments been made against the loan balances.

15. Based on my review of U.S. Customs and Border Protection records, I have learned that the purported applicants for the 17 Alias EIDL Applications had all previously traveled to the United States and then left before the onset of the COVID-19 virus in or about March 2020. The travel records show that the purported applicants were not in the United States when the applications were submitted in or around June and July 2020. This means the statements on the applications listing owner/applicant addresses in the United States were false.

16. Based on my search of bank records and driver's license records, I have learned the following:

a. Each of the 17 Alias EIDL Applications lists a bank account at Wells Fargo into which the SBA loan funds should be sent (the "17 Alias Bank Accounts"). The bank accounts were

frequently created just days before the applications were submitted.

b. For each of the 17 Alias Bank Accounts, the account opening documents list a driver's license for the purported owner of the bank account, whose name matches the EIDL applicant.

c. An FBI agent searched driver's license records and found that the results further confirmed that the aliases were used fraudulently. Specifically, in many instances, the driver's license information listed in the 17 Alias Bank Account opening documents did not come back to any individual. Put another way, a search for the driver's license information did not yield any results. Based on my training and experience, I believe this means the driver's license information was not genuine and did not actually belong to the applicant. In the remaining instances, a search for the driver's license information returned a person other than the purported EIDL applicant and bank account owner. Based on my training and experience, both scenarios are consistent with the 17 Alias EIDL Applications being fraudulent applications.

17. The table below reflects the information I learned from reviewing SBA records and Wells Fargo Bank records:

EIDL Loan Applicant and Bank Account Owner	Loan Amount[2]	Bank Account (Last Four Digits)	Date Bank Account Opened	Date Loan App. Submitted	Date Loan Funds Posted
Individual R.B.	$159,900	9526	2/24/2020	6/27/2020	6/30/2020

[2] The "Loan Amount" includes the SBA loan advance. The "Date Loan Funds Posted" means the date the SBA loan advance or the primary SBA loan posted, whichever is earlier.

EIDL Loan Applicant and Bank Account Owner	Loan Amount[2]	Bank Account (Last Four Digits)	Date Bank Account Opened	Date Loan App. Submitted	Date Loan Funds Posted
Individual S.D.	$158,900	2271	6/30/2020	6/30/2020	7/7/2020
Individual E.J.	$149,900	4471	4/21/2018	7/20/2020	7/22/2020
Individual O.K.	$149,900	6568	7/15/2020	7/15/2020	7/21/2020
Individual A.B.	$157,900	7616	10/22/2019	7/8/2020	7/10/2020
Individual A.C.	$157,900	6299	2/19/2020	7/6/2020	7/8/2020
Individual A.S.	$159,900	9048	6/29/2020	6/29/2020	7/7/2020
Individual P.P.	$157,900	9283	6/30/2020	7/1/2020	7/6/2020
Individual A.T.	$157,900	2430	6/29/2020	6/29/2020	7/7/2020
Individual I.A.	$152,900	8001	2/23/2020	7/7/2020	7/9/2020
Individual I.K.	$159,900	9384	6/30/2020	6/30/2020	7/7/2020
Individual S.P.	$149,900	3084	7/10/2020	7/14/2020	7/21/2020
Individual K.A.	$149,900	7153	7/15/2020	7/15/2020	7/21/2020
Individual D.B.	$149,900	0372	6/30/2020	7/17/2020	7/21/2020
Individual A.D.	$149,900	1272	7/15/2020	7/15/2020	7/21/2020
Individual S.S.	$149,900	3806	7/15/2020	7/15/2020	7/21/2020
Individual T.S.	$142,900	6761	6/30/2020	6/30/2020	7/23/2020

18. Based on my training and experience, the pattern of opening bank accounts shortly before the applications were submitted is consistent with the business being sham entities. That is, they did not do genuine business, which often requires an operating bank account. This is particular true for the lucrative purported business that, according to the 17 Alias EIDL Applications, had incomes of hundreds of thousands of dollars each year.

19. Based on my review of bank records, I have learned the following:

a. As a result of the 17 Alias EIDL Applications, the SBA disbursed a total of approximately $2,615,300 into the 17 Alias Bank Accounts. As set forth above, the bank accounts were created days before the relevant EIDL application was

submitted. Soon after the loan funds were disbursed by the SBA, money was routed to various sources that, based on my training and experience, are inconsistent with the purpose of SBA loans and support the conclusion that the 17 Alias EIDL Applications were fraudulent.

b. The 17 Alias Bank Accounts received few funds into the accounts except for SBA loan disbursements. Accordingly, the outflows from those accounts, described below, are principally from SBA loan money disbursed based on the 17 Alias EIDL Applications.

c. The largest percent of money from the 17 Alias EIDL Applications went to a set of business bank accounts at First Bank for which MEHRRAFIEE is the loan authorized signer. MEHRRAFIEE's business bank accounts are listed below[3]:

Account Holder	Bank & Last Four Digits of Account Number	Authorized Signer(s)	Amount Received from the 17 Alias Bank Accounts
Platinum Entertainment Group	First Bank x1310	MEHRRAFIEE	$439,525
Exotic Secrets LLC	First Bank x6646	MEHRRAFIEE	$454,856
American Golden Coverage Brokers	First Bank x4390	MEHRRAFIEE	$405,389
I Concert Entertainment Inc	East West Bank x2916	MEHRRAFIEE	$46,210
Café Taraneh Inc	First Bank x6164	MEHRRAFIEE	$171,710
Laa Group Inc	First Bank x3733	MEHRRAFIEE	$179,100
Atila Investments	First Bank x8545	MEHRRAFIEE	$54,220

[3] Based on my review of bank records, I know there were frequent transfers back-and-forth between different accounts controlled by MEHRRAFIEE. The transfer amounts listed below are the net amount of the transfers from the 17 Alias Bank Accounts to the relevant MEHRRAFIEE business account.

Account Holder	Bank & Last Four Digits of Account Number	Authorized Signer(s)	Amount Received from the 17 Alias Bank Accounts
Lux Dental Spa	First Bank x2338	MEHRRAFIEE, Laleh Mehrrafiee	$45,775
Wilshire Center Insurance Services	First Bank x3953	MEHRRAFIEE	$24,300
Road Ad	First Bank x9096	MEHRRAFIEE	$47,700

d. In addition, significant sums of money went from the 17 Alias Bank Accounts to luxury goods and brokerage accounts that have no apparent business purpose:

i. Approximately $335,540 was spent in checks addressed to "Luxury Watch" or "Luxury Watch Co."

ii. Approximately $152,946 went to Coinbase, a popular cryptocurrency platform. Approximately $15,280 went to Fidelity Brokerage Services, which is a popular investment platform.

iii. Approximately $96,773 was withdrawn in cash or written to checks that were cashed.

20. In addition to the 17 Alias EIDL Applications described above, bank records show that the MEHRRAFIEE Business Bank Accounts received significant funds – approximately $2 million – from approximately 10 other aliases that received EIDL and PPP loans. I have requested the relevant EIDL and PPP loan applications, as well as corresponding bank account records, and the FBI is continuing to analyze those records to link MEHRRAFIEE to additional suspected fraudulent EIDL applications.

D. MEHRRAFIEE Exchanged Text Messages With Others About Submitting Fraudulent Applications and Using the 17 Aliases

21. As set forth below, law enforcement officers obtained a search warrant for MEHRRAFIEE's Apple iCloud account. Apple iCloud records showed many text message records showing MEHRRAFIEE's knowledge of the false statements on the EIDL applications that benefitted him and using the 17 fraudulent aliases.

22. On or about November 13, 2024, the Hon. Jean P. Rosenbluth, United States Magistrate Judge, authorized warrants to seize and search various online accounts. The online accounts included the Apple iCloud account shirzadmusic@yahoo.com (the "MEHRRAFIEE iCloud Account") and the Yahoo and Google accounts shirzadrafiee@yahoo.com, shirzadmusic@yahoo.com, rocky_fit@yahoo.com, shirzadmusic@gmail.com, and secretsexotic@gmail.com (the "MEHRRAFIEE Email Accounts").

23. Based on my review of Apple records, I have learned the following:

a. The MEHRRAFIEE iCloud Account is subscribed to in the name of "Shirzad Rafiee." The email address associated with the account references MEHRRAFIEE's first and last name. Based on my review of Apple iCloud records, I have seen many photographs of MEHRRAFIEE in the Apple iCloud records, consistent with the account being frequently used by MEHRRAFIEE.

b. On or about May 16, 2020, MEHRRAFIEE, using a particular phone number ending in 8353 (the "MEHRRAFIEE Phone

Number"),[4] exchanged text messages with the user of a phone number ending in 0202 ("CC-1"). Among other things, MEHRRAFIEE gave CC-1 instructions on what information to include on a disaster loan application. MEHRRAFIEE told CC-1 to "[m]ake sure that the cost of goods is only 40% of your gross" and "[j]ust put that you have 10 employees." When MEHRRAFIEE was asked what numbers to put on the form, he responded "Between $125K to 135K."

c. On several dates in 2020, MEHRRAFIEE, using the MEHRRAFIEE Phone Number, exchanged text messages with the user of a phone number ending in 9676 ("CC-2"):

i. On or about August 4-5, 2020, CC-2 wrote "Bro re deposit check from [Individual A.D.] for the $500." Later, CC-2 wrote, "U need to tell me which ones ur doing and when. I can't keep 20 phones on me." MEHRRAFIEE responded "Okay."

ii. On or about September 10, 2020, CC-2 wrote, "[d]id you do [Individual P.P.]" and "[l]ast transaction is showing Sept 02 for $28k." Based on my review of bank records, the last transaction prior to September 10, 2020, in the bank account in the name of Individual P.P. was a check for $28,000, dated September 2, 2020, addressed to "American Golden Coverage Brokers." As set forth above, American Golden Coverage Brokers is another business account controlled by MEHRRAFIEE.

---

[4] Based on my review of T-Mobile Records, I have learned that MEHRRAFIEE is the subscriber for the 8353 Phone Number. Records from T-Mobile show that on or about June 6, 2022, the 8353 Phone Number, subscribed to MEHRRAFIEE, was "ported in" from another phone provider.

iii. On or about September 11, 2020, CC-2 wrote, "Ima send u a list of ones that r done," and he sent a list of names including Individuals I.K., A.S., P.P., S.D., and A.T.

iv. On or about October 15, 2020, CC-2 wrote to MEHRRAFIEE saying "[f]inish these 3 please" and listing three names including Individual A.C. Next to the name for Individual A.C., CC-2 wrote "$20k finish."

v. On or about September 14, 2020, CC-2 wrote to MEHRRAFIEE with a list of first names, last initials, and dollar amounts, including "[Individual O.K.] 53k," and "[Individual S.S.] $88k." CC-2 added "These r getting close. Can u finish them by next week?" MEHRRAFIEE responded, "Oh yes for sure." CC-2 said "Bro did u do the $10k for [Individual O.K.] cause it's still not showing?" MEHRRAFIEE wrote back, "Yes bro" and "It will show tomorrow."

vi. On or about October 12, 2020, MEHRRAFIEE and CC-2 exchanged a series of message discussing a person who can "make" driver's licenses. MEHRRAFIEE and CC-2 specifically discuss what the prefix that should start the driver's license number, with different prefixes corresponding to different immigration statuses.

vii. Based on my training and experience, I believe the messages above reflect MEHRRAFIEE engaging in the scheme to submit fraudulent EIDL aliases and then aiding CC-2 in depleting the bank accounts of the SBA loan money.

d. In or about April 2021 and May 2021, MEHRRAFIEE, using the MEHRRAFIEE Phone Number, exchanged text messages with

the user of a phone number ending in 9304 ("CC-3"). On or about April 21, 2021, CC-3 wrote to MEHRRAFIEE to "bring all the plastic id's please," to which MEHRRAFIEE responded "[r]elax ok bro" and "[t]hey are in the middle of getting things done." Based on my training and experience, including my awareness of fraud schemes, I believe the referenced "plastic ids" are fake identification cards. On or about April 29, 2021, CC-3 sent MEHRRAFIEE a list of several names, including the ones for Individuals A.C., A.B., A.D., A.T., P.P., K.A. and S.S." CC-3 added, "I emailed everything."

e. In or about April 2021, MEHRRAFIEE, using the MEHRRAFIEE Phone Number, exchange text messages with the user of a phone number ending 2723 ("CC-4"). In one text message exchange on or about April 27, 2021, MEHRRAFIEE wrote to CC-4, saying "Plz sign the applications for these:" and listing three surnames. CC-4 wrote back saying "I already signed these back on April 23rd."

E. MEHRRAFIEE's Fraudulent EIDL Applications In His Own Name

24. As set forth below, in addition to the 17 Alias EIDL Applications described above, MEHRRAFIEE also submitted an EIDL application to the SBA for a business he controls that contained misrepresentations. In the application, MEHRRAFIEE claimed he had no prior felony conviction, which is false given that he has a federal felony conviction for presenting fake documents to a bank when applying for a loan. Later, MEHRRAFIEE submitted another EIDL application for the same business listing different

revenue, cost of goods sold, and a different number of employees.

1. The Fraudulent I Concert EIDL Application Yields $150,000

25. Based on my review of SBA records, I have learned the following:

a. On or about March 30, 2020, an EIDL application was submitted for the business "I Concert Entertainment LLC," with a Tax ID number ending in 2160 ("I Concert EIDL Application-1"). On the application, MEHRAFIEE is listed as the sole owner of the business, and the application is signed by "Shirzad Mehrafiee." MEHRRAFIEE listed the email address shirzadrafiee@yahoo.com. Based on my review of Yahoo records, I know that this email address is subscribed to "shirzad Rafiee," which I believe is a reference to MEHRRAFIEE's first name and last name. With his EIDL application, MEHRRAFIEE also submitted an image of his United States Permanent Resident card, which matches MEHRRAFIEE's appearance based on driver's license records.

b. In I Concert EIDL Application-1, MEHRRAFIEE listed $650,000 as the business's gross revenue and $150,000 as the cost of goods. The number of employees listed on the application was 4.

c. MEHRRAFIEE answered "no" to the Criminal History Question.

d. On or about April 17, 2020, the SBA approved an advance of $4,000, and the next day it disbursed that amount to MEHRRAFIEE.

e. On or about May 19, 2020, the SBA approved the application and authorized a loan in the amount of $150,000. On or about the same day, MEHRRAFIEE electronically signed a Loan Authorization and Agreement, along with a related Security Agreement, on behalf of I Concert Entertainment LLC. In those agreements, among other representations, MEHRRAFIEE certified that "Borrower will use all proceeds of this loan solely as working capital to alleviate economic injury caused by disaster occurring in the month of January 31, 2020 and continuing thereafter," and "none of the Obligations are or will be primarily for personal, family, or household purposes."

f. The Loan Authorization and Agreement also included a reminder that "any false statement or misrepresentation to SBA may result in criminal, civil or administrative sanctions including, but not limited to . . . fines, imprisonment or both . . . ."

g. MEHRAFIEE electronically signed the Loan Authorization and Agreement under penalty of perjury and certified that he was authorized to apply for and obtain a disaster loan on behalf of I Concert Entertainment LLC "in connection with the effects of the COVID-19 emergency."

h. On or about May 19, 2020, the SBA disbursed approximately $149,900 in loan proceeds into a bank account at

First Bank ending in 7630 ("Bank Account-1").[5] This was the same bank account into which the $4,000 EIDL advance was disbursed on or about April 18, 2020.

26. Based on my review of records from First Bank, I have learned the following:

a. MEHRRAFIEE opened Bank Account-1 on or about March 25, 2020, *i.e.*, just five days before he submitted I Concert EIDL Application-1. MEHRRAFIEE is listed as the sole signer for the checking account and used his Missouri Driver's License, number ending in 866, as his proof of identity (the "Missouri ID Number"). First Bank maintained a copy of this driver's license on file, which I have reviewed, and the photo shows the appearance of MEHRRAFIEE based on a comparison to law enforcement photographs and the driver's license submitted with I Concert EIDL Application-1.

b. Within approximately two days from receiving the loan of $149,900, MEHRRAFIEE wrote two checks out of this bank account:

i. *First*, on or about May 21, 2020, MEHRRAFIEE wrote a check for $125,000 to "LAA Group." As set forth below, bank records show this check was deposited into another bank account operated by MEHRRAFIEE with account number ending in 8545.

ii. *Second*, on or about May 21, 2020, MEHRRAFIEE

[5] Based on my review of publicly available information about the EIDL program, I have learned that the SBA charges a fee of $100 for EIDL loans over $25,000. Accordingly, the loan disbursement of $149,900 accounts for the $150,000 loan minus the $100 fee.

wrote a check for $24,000 to "I Concert Entertainment." Bank records show this check was deposited into another bank account operated by MEHRRAFIEE with account number ending in 6164, discussed further below.[6]

27. Based on my review of First Bank records, I have learned the following:

a. On or about April 22, 2020, MEHRRAFIEE opened a bank account in the name of "Laa Group Inc." at First Bank, and the account was assigned a bank account number ending in 545 ("Bank Account-2"). MEHRRAFIEE was the sole signer on Bank Account-2.

b. On or about May 21, 2020, MEHRRAFIEE deposited the above-described $125,000 check into Bank Account-2. The next day, on or about May 22, 2020, MEHRRAFIEE wrote a $9,000 check that was addressed to himself. Between June 5, 2020, and June

[6] Based on my review of California Secretary of State records, I have learned that MEHRRAFIE established another purported business with a similar name, "I Concert Entertainment Inc.", in California on April 19, 2021. MEHRRAFIEE is listed on these records as the Chief Executive Officer ("CEO"), the Secretary, and the Chief Financial Officer ("CFO"). The business address is 17530 Ventura Blvd., Suite 203, Encino, California 91316 (the "Ventura Blvd. Address"). The business type is listed as "Entertainment." Based on my review of records from the Missouri Secretary of State, the purported business "I Concert Entertainment LLC," charter number LC001539246, was established by MEHRRAFIEE on or about May 31, 2017. The articles of incorporation list the business address as 2516 SW Valley Ridge Lane, Lees Summit, Missouri 64082 (the "Valley Ridge Lane Address") and the email address i.concert@yahoo.com. Based on my review of information obtained from Yahoo, i.concert@yahoo.com was registered by "I concert," with the verified recovery phone number as the 8353 Phone Number. A review of MEHRRAFIEE's credit records indicate that MEHRRAFIEE lived at the Valley Ridge Lane Address from approximately March 2011 until March 2018.

22, 2024, MEHRRAFIEE wrote three checks from Bank Account-2 that were made to "Cash." Each of these four checks has a signature that was similar to MEHRRAFIEE's signature on the Bank Account-2 signature card.[7]

2. MEHRRAFIEE Obtains An Additional $350,000 In Loan Money Through A Loan Modification

28. Based on my review of publicly available information about the EIDL program, I have learned that individuals who have obtained EIDL loans may apply for a loan modification, which can increase the value of the loan to which they are entitled.

29. Based on my review of SBA records, I have learned the following:

a. On or about May 3, 2021, MEHRAFIEE requested a modification of I Concert EIDL Application-1 to increase the loan amount from $150,000 to $500,000. As reflected in notes from the SBA's records, MEHRRAFIEE told the SBA the following: "I am requesting more funding for my business and I have had a very large percentage of business lost due to Covid and I am NOT in any bankruptcy. I have changed my bank so I just need to update with new information."

b. Between May 2021 and December 2021, MEHRRAFIEE called the SBA several times to check in on the status of his loan.

[7] Based on my review of California Secretary of State records, LAA Group Inc., is a purported advertising business owned by MEHRRAFIEE and registered to the Ventura Blvd. Address.

c. On or about January 7, 2022, the SBA approved the request and authorized a loan modification, increasing the total loan amount to $500,000.

d. On or about January 7, 2022, MEHRRAFIEE electronically signed a new Loan Authorization and Agreement, along with a related Security Agreement, on behalf of I Concert Entertainment LLC.[8] In those agreements, among other representations, MEHRRAFIEE certified that "Borrower will use all proceeds of this loan solely as working capital to alleviate economic injury caused by disaster occurring in the month of January 31, 2020 and continuing thereafter," and "None of the Obligations are or will be primarily for personal, family, or household purposes."

e. MEHRAFIEE electronically signed the Loan Authorization and Agreement under the penalty of perjury and certified that he was authorized to apply for and obtain a disaster loan on behalf of I Concert Entertainment LLC "in connection with the effects of the COVID-19 emergency."

f. On or about January 20, 2022, the SBA disbursed an additional $350,000 to East West Bank account 2916 ("Bank Account-3").

30. Based on my review of East West Bank records, I have learned the following:

[8] Each application appeared to be for I Concert Entertainment LLC as they included the EIN and ownership information for that purported business. One application, however, did not include the "LLC" designation in the business name.

a. Bank Account-3 was opened by MEHRRAFIEE on or about April 27, 2021. MEHRRAFIEE is the only authorized signer on the account. In bank records, MEHRRAFIEE listed himself as the Chief Executive Officer of I Concert Entertainment Inc., d/b/a "Shirzad Music."

b. Bank Account-3 had approximately $213,000 prior to the EIDL disbursement of $350,000. The EIDL loan funds were pre-authorized and available for use on January 12, 2022. On or about January 14, 2022, $10,465 was used to pay a Barclay Credit Card. Records from Barclays show that MEHRRAFIEE paid this amount on his personal credit card at Barclays. On or about January 20, 2022, two checks were written totaling $100,000 to a consulting business. An additional two checks for $100,000 were written to the same business on or about January 24, 2022. During that same time, two inter-account transfers were completed totaling $86,000 to MEHRRAFIEE's East West Bank accounts for Lux Dental Spa and Advva.

c. Bank records show several transactions soon after the loan deposit that are inconsistent with MEHRRAFIEE's representations about how the loan funds would be used:

i. On or about January 20, 2022, $20,000 was transferred from Bank Account-3 to another business bank account MEHRRAFIEE controlled, namely an account at East West Bank in the name of "Advva" ending in account number 2866 ("Bank Account-4"). Bank records show that MEHRRAFIEE is the only authorized signer for Bank Account-4. The bank account was opened on or about April 21, 2021.

ii. On or about January 14, 2022, MEHRRAFIEE used $10,465.87 to a pay his credit card at Barclays Bank. Based on my review of Barclays Bank records, I have learned that Barclays Bank is the provider of a Luxury Card Credit card in the name of "Shirzad Mehrrafiee." Barclays records do not make any reference to this Luxury Card credit card being associated with any business.

iii. Between on or about January 21, 2022 and January 31, 2022, MEHRRAFIEE transferred $5,827 to a bank account at Goldman Sachs Bank. Based on my review of Goldman Sachs Bank records, I have learned the Goldman Sachs Bank is the provider of an Apple credit cards in the name of "Shirzad Mehrrafiee." Goldman Sachs Bank records do not make any reference to this Apple credit card being associated with any business.

iv. On or about February 16, 2022, MEHRRAFIEE transferred $9,875 to a bank account at JPMorgan Chase Bank. Based on my review of JPMorgan Chase Bank records, I have learned that JPMorgan Chase is the provider of a Chase Freedom credit card in the name of "Shirzad Mehrrafiee." JPMorgan Chase records do not make any referees to this Chase Freedom credit card being associated with any business.

v. On or about January 5, 2022, MEHRRAFIEE made a payment from Bank Account-3 to "Ventura County Water and Sanitation" for approximately $1,037. Based on my training and experience, I believe this may be a water and/or sanitation utility payment. None of MEHRRAFIEE's purported businesses are

located in Ventura County, California. However, MEHRRAFIEE's home, SUBJECT PREMISES-2, is located in Ventura County.

vi. On or about January 28, 2022, MEHRRAFIEE sent a wire for $8,000 to "Cocolalla Creek Sport Horses." Based on my review of their website, on October 24, 2024, Cocolalla Creek Sport Horses is a horse farm located in Cocolalla, Idaho.

vii. Based on my training and experience, the transactions described above from Bank Account-3 soon after the $350,00 EIDL loan deposit are inconsistent with the operation of the "entertainment services" business purportedly operated by MEHRRAFIEE and the purposes for which he was permitted to use EIDL money.

3. MEHRRAFIEE Applies For another EIDL Loan for I Concert Entertainment, Now Listing Different Information

31. Based on my review of SBA records, I have learned the following:

a. On or about February 15, 2021, MEHRRAFIEE submitted another EIDL application for I Concert Entertainment LLC. The application listed $1,018,753 as the business's gross revenue and $550,618 as the cost of goods. The number of employees listed on the application was twelve. The gross revenue, cost of goods, and number of employees were all different when compared to I Concert EIDL Application-1,

described above. However, the information should be the same as both applications ask for that data for the same time periods.[9]

b. By the time of I Concert EIDL Application-2, the SBA had modified the text of the Criminal History Question to ask only whether the applicant had been convicted of any felony crimes in the past five year. MEHRRAFIEE accurately answered that he had not been so convicted.

c. Both applications were certified by MEHRRAFIEE as "true and accurate" under the penalty of perjury. Unlike the prior application, however, the SBA denied this EIDL application.

F. MEHRRAFIEE Applied for a Mortgage for SUBJECT PREMISES-2 By Overstating His Income and Using a Fake Bank Statement

32. As set forth below, in 2021, MEHRRAFIEE applied for and received a home mortgage loan worth approximately $3 million to purchase SUBJECT PREMISES-2. However, he inflated his monthly income, and his claim on the mortgage form is contradicted by tax records. In addition, MEHRRAFIEE submitted a false bank statement that grossly inflated his assets.

33. Based on my review of bank records, I have learned the following:

[9] Based on my review of SBA records, I have learned that the SBA obtained tax records from the IRS for I Concert Entertainment LLC in connection with its review of I Concert Application-1. Among other things, a tax transcript for 2019 shows gross receipts of $1,077,967 and Cost of Goods Sold of $550,618. Accordingly, compared to the tax transcript, the numbers listed in I Concert Application-1 understates the business's purported gross receipts and understates its Cost of Goods Sold. By contrast, the numbers listed in I Concert Application-2 more closely reflect the figures in the tax transcript.

a. On or about June 28, 2021, MEHRRAFIEE applied for a home mortgage at Fifth Street Capital for the property at SUBJECT PREMIES-2. There was no listed co-borrower. MEHRRAFIEE applied for a loan of $2,919,000, providing the rest of the purchase price in cash. The property has an appraised value of approximately $4.2 million.

b. In his application, MEHRRAFIEE listed his employment as the owner of I Concert Entertainment, LLC, and he did not list any other employer or self-employed business. He listed his gross monthly base employment income as $179,369.05. However, this amount is contradicted by tax records.

c. Specifically, based on my review of records provided by the California Franchise Tax Board, I know that MEHRRAFIEE submitted a copy of the I Concert Entertainment, LLC Form 1120-S for tax year 2021, labeled the "U.S. Income Tax Return for an S-Corporation" (the "I Concert Form 1120-S"). On the form, MEHRRAFIEE is listed as the 100% shareholder in the business. MEHRRAFIEE listed the business's annual gross receipts or sales for 2021 as $398,506 – far less than the monthly gross income MEHRRAFIEE claimed on his mortgage application. I have also seen Form 1040s submitted by MEHRRAFIEE to the California Franchise Tax Board. For 2020, MEHRRAFIEE listed total income of $74,127, which was drawn from rental real estate, royalties, partnerships, S-corporations, or trusts. For 2021, MEHRRAFIEE listed total income of $78,459 from the same sources. Accordingly, MEHRRAFIEE's Form 1040s also list significantly

lower income than what MEHRRAFIEE claimed on his home mortgage application.

d. Fifth Street Capital's mortgage files include bank statements that purportedly reflect MEHRRAFIEE's income (the "Mortgage File Bank Statements"). The bank statements purportedly show the monthly statements between June 2020 to April 2021 for a First Street Bank account in the name of "I Concert Entertainment LLC" with account number ending in 6164 ("Bank Account-5"). I have reviewed monthly bank statements for the same account and the same time period that were obtained from First Street Bank (the "Genuine Bank Statements").

e. By comparing the Mortgage File Bank Statements to the Genuine Bank Statements, I have learned that the monthly Mortgage File Bank Statements purporting to show January 2021 to April 2021 were false. The false bank statements contain many of the same entries as the genuine bank statements; however, they also contain entries that substantially inflate the assets and income into the accounts. For example, the genuine April 2021 statement lists the beginning balance as $216,542.45 and the false version in the mortgage file lists the beginning balance as $1,516,542.45. In some instances, the change was as simple as adding a digit. In the same bank statements, the monthly "total additions" on the genuine statement is $55,297.51 and the same figure on the false statement is $255,297.51.

f. Below is a comparison of the genuine monthly statement for March 2021 and the false statement for March 2021 in the mortgage file:

Business First Checking

Account number	XXXXXX6164	Beginning balance	$264,710.25
Enclosures	10	Total additions	345,880.00
Low balance	$26,529.41	Total subtractions	394,047.80
Average balance	$107,950.12	Ending balance	$216,542.45
Avg collected balance	$99,399		

CHECKS

Number	Date	Amount	Number	Date	Amount
2081	03-05	6,552.00	2083	03-12	528.00
2082	03-22	442.00	2084	03-15	50.00

DEBITS

Date	Description	Subtractions
03-01	' POS Purchase MERCHANT PURCHASE TERMINAL 55488721 JERSEY MIKES 20116 ENCINO CA XXXXXXXXXXXX1424	29.52
03-01	' ACH Withdrawal EPX ST 032062426 MERCH SETL 210301 3130032062426	2.97
03-02	' ACH Withdrawal EPX FE 032062426 MERCH SETL 210302 3130032062426	71.90

Genuine March 2021 Statement from First Street Bank

Business First Checking

Account number	XXXXXX6164	Beginning balance	$1,264,710.25
Enclosures	10	Total additions	645,880.00
Low balance	$1,226,529.41	Total subtractions	394,047.80
Average balance	$1,407,950.12	Ending balance	$1,516,542.45
Avg collected balance	$1,299,399		

CHECKS

Number	Date	Amount	Number	Date	Amount
2081	03-05	6,552.00	2083	03-12	528.00
2082	03-22	442.00	2084	03-15	50.00

DEBITS

Date	Description	Subtractions
03-0 1	' POS Purchase MERCHANT PURCHASE TERMINAL 55488721 JERSEY MIKES 20116 ENCINO CA XXXXXXXXXXXX 1424	29.52
0301	1 ' ACH Withdrawal EPX ST 032062426 MERCH S ETL 210301 3130032062426	2.97
0302	' ACH Withdrawal EPX FE 032062426 MERCH SETL 210302 3130032062426	71.90

False March 2021 Statement from the Fifth Street Capital Mortgage File

g. Fifth Street Capital records show that the company approved MEHRRAFIEE's loan application. On May 17, 2021,

MEHRRAFIEE signed the purchase agreement for the property as the owner buyer. On or about June 2, 2021, MEHRRAFIEE signed the note for the mortgage loan from Fifth Street Capital.

34. Based on my review of court records, I know that MEHRRAFIEE was previously convicted and sentenced to two years in prison for a similar loan fraud scheme in which he use fake documents to obtain loans. *See* Plea Agreement at 2, *United States v. Mehrrafiee et al.*, No. 06-cr-310-W-SOW (W.D. Mo.), Dkt. 44 (defendant admitting, as factual basis for the plea, that he, "in agreement with others, knowingly and willfully provided banks and mortgage lending companies with fraudulently altered federal tax returns, pay stubs, W-2 wage statements, identification, and automobile titles (representing inaccurate milage statements), thereby causing the banks to rely on the false information in providing funds to the defendant and others.").

G. MEHRRAFIEE's Kiting Scheme Results In East West Bank Losing Approximately $1.5 Million

35. As set forth below, in or around October 2024, there is evidence showing that MEHRRAFIEE and another individual who lives with him ("Individual-1") conducted a kiting scheme at East West Bank.[10] The scheme involved sending large wire transfers back-and-forth between accounts at East West Bank and Citizens Business Bank. As a result of the scheme, East West

[10] As set forth below, a staff member at East West Bank believed MEHRRAFIEE and Individual-1 are married. Based on my investigation, I do not believe MEHRRAFIEE and Individual-1 are formally married. However, I do believe Individual-1 lives with MEHRRAFIEE at SUBJECT RESIDENCE-2; for example, Individual-1's driver's license has the address for SUBJECT RESIDENCE-2.

Bank has lost a total of approximately $1.5 million. In a statement to the bank, MEHRRAFIEE claimed that people owed him money and checks simply bounced but, based on my training and experience, that is inconsistent with the deliberate scheme executed by MEHRRAFIEE and his co-conspirator.

36. Based on my review of FBI complaint referral records, I have learned the following:

a. On or about October 17, 2024, an employee at East West Bank in Los Angeles, California (the "Bank Employee"), reported to the FBI that East West Bank had been the victim of a kiting scheme in which the bank lost approximately $2,186,000. As set forth below, the bank was later able to recoup some of its loss and is currently facing a total loss of approximately $1.5 million. Based on my training and experience, I know that a kiting scheme is a common bank fraud scheme in which an individual sends a check or wire from one account without adequate funds into a second account. When the second account is funded with the check or wire, the user then withdraws money from the second account. When the bank realizes that the check or wire was inadequate, the bank can reverse that check or wire, but money has already disbursed money to the schemer so the bank must typically bear the loss from the withdrawal out of the second bank account. Kiting schemes can involve multiple transfers and multiple bank accounts.

b. The Bank Employee reported that the resulting wires in the fraud were recalled on or about October 16, 2024. The Bank Employee reported that the subjects of the bank's

investigation, who the bank believed committed the fraud, were MEHRRAFIEE and Individual-1, who the bank believed were a husband and wife pair.

c. The Bank Employee affirmed that the information was true and accurate to the best of his/her knowledge, and acknowledged that a false statement could subject him/her to a fine, imprisonment, or both.

37. On or about December 31, 2024, I interviewed the Bank Employee. During that interview, the Bank Employee reported, among other things, the following:

a. The Bank Employee is a Fraud Investigation Supervisor in the Risk and Operations Department at East West Bank. The Bank Employee submitted the crime report to the FBI because MEHRRAFIEE, Individual-1, and their various business accounts have caused a loss to East West Bank.

b. At the time of the interview, the accounts for both MEHRRAFIEE and Individual-1 were negative. MEHRRAFIEE's total balance at East West Bank was approximately -$579,000 and Individual-1's was approximately -$918,000. MEHRRAFIEE told East West Bank that he and Individual-1 are not married and not related, but East West Bank believed they are married since they have children together and live at the same address.

c. East West Bank was in the process of closing MEHRRAFIEE's bank accounts due to suspicious activities. MEHRRAFIEE had many checks going back and forth between East West Bank and Citizens Business Bank. MEHRRAFIEE overdrew his accounts on the same day that East West Bank was scheduled to

close them. MEHRRAFIEE deposited multiple checks that day and wanted to wire the funds the same day to Citizens Business Bank. Since the accounts were scheduled to close that day, the holding period for the checks were waived and the wires were approved. The same month that MEHRRAFIEE was told East West Bank would be closing his accounts, Individual-1 opened her accounts at East West Bank.

d. MEHRRAFIEE told the bank that he would pay back the funds. He stated that many people owed him money and their checks were bouncing. Individual-1 gave a similar story to the bank, saying that they work in the entertainment industry and that many people owe them money. MEHRRAFIEE has made a few small deposits since the bank closed his accounts and has been to the local branch as recently as November.[11]

38. Based on my review of Citizens Business Bank records, I have learned that the bank records from Citizens Business Bank are consistent with the complaint submitted by East West Bank as the victim of a kiting scheme. The bank wires referenced in the East West Bank FBI complaint match the Citizens Business Bank records. Among other thing, between approximately September 2024

[11] In addition, the Bank Employee stated that MEHRRAFIEE is well known by all of the employees at his/her local East West Bank branch. All of the employees knew him and his business well. He is flamboyant and very sociable. He held himself out as working in the entertainment business, which he expressed to employees can be risky financially. He would regularly deposit large numbers of checks and cash. All of his transactions took place at the local branch. MEHRRAFIEE often worked with the managers at the local East West Bank branch. The holding period for checks depends on the bank. They could be varied based on the relationship of the customer and bank. The branch managers and assistant branch managers have the ability to override the standard hold periods on various transaction types.

and October 2024, Citizens Business Bank records show frequent six-figure transfers back-and-forth with accounts at East West Bank. Based on my training and experience and my communication with an FBI financial analyst, I believe this is an unusual pattern of transactions. Given East West Bank's significant loss incurred over a short period of time, I believe the pattern is consistent with a kiting scheme.

H. MEHRRAFIEE's Money Laundering and Unlicensed Money Transmitting Scheme

39. As set forth below, bank records show that between approximately 2020 and 2024, MEHRRAFIEE deposited approximately $48 million in cash and checks into a small handful of bank accounts he controlled. Law enforcement officers conducting surveillance saw him meet with individuals at various locations in the southern California area and pick up packages from those people, which agents believe to be money pickups. In a handful of instances, agents saw MEHRAFIEE meet with a particular individual who was arrested three days ago for his role in a scheme to launder $150,000 from a fraud victim in Tennessee. Toll records show frequent WhatsApp communications between MEHRAFFIEE and the recent arrestee.

1. MEHRRAFIEE Deposits Approximately $48 million in Cash and Checks Over a Four Year Period.

40. Based on my review of bank records, I have learned the following:

a. Six businesses deposited or cashed 232 checks for approximately $9.1 million deposited at Hermanos 3 Mercado.

Based on my review of publicly available information, I have learned that Hermanos 3 Mercado is a check cashing business.

b. MEHRRAFIEE wrote checks to approximately 1,460 individuals for a total of approximately $42.9 million. Of that total, approximately $5.5 million went to 20 individuals.

c. Over the previous four years MEHRRAFIEE made approximately 686 credit card payments for a total of approximately $3.16 million. MEHRRAFIEE spent approximately $1.4 million on automobiles.

d. MEHRRAFIEE made approximately $1.3 million in withdrawals and transfers with bank tellers.

e. MEHRRAFIEE made approximately $2.45 million in escrow, mortgage and real estate transactions.

41. On or about February 9, 2025, I searched on U.S. Department of the Treasury FinCEN's publicly available portal for money service business registration.[12] I searched for MEHRRAFIEE's name as well as the names of his known businesses, listed above, and I did not find any registered money service businesses.

2. MEHRRAFIEE Met with a Co-Conspirator, Who Was Later Charged and Arrested for Fraud, and then Deposited Large Quantities of Cash

42. Based on my review of FBI surveillance reports, I have learned the following:

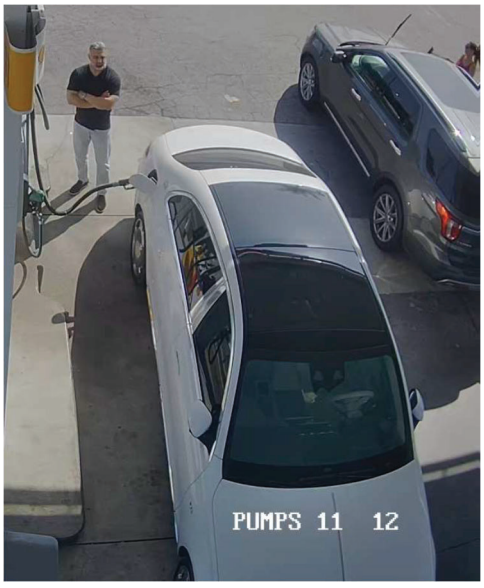
a. On or about September 24, 2024, FBI Special Agents conducting surveillance saw MEHRRAFIEE driving in a white Mercedes Maybach, California license plate 9LCT781, *i.e.*, the

[12] *See* https://www.fincen.gov/msb-state-sele.ctor.

SUBJECT VEHICLE.[13] MEHRRAFIEE, driving the SUBJECT VEHICLE, pull into a gas station in Encino, California. After filling his gas tank, MEHRRAFIEE got into his car and waited.

b. Another vehicle then pulled up at the next gas pump ("Vehicle-1"). The driver exited the vehicle with a plastic bag and gave the bag to MEHRRAFIEE. The driver then re-entered their vehicle and drove away from the gas station. Based on my review of vehicle registration records, I know that Vehicle-1 is registered to Mahdi Rajabi. The driver of Vehicle-1 also matched the appearance of Rajabi, based on my review of surveillance records and a driver's license photograph of Rajabi.[14]

c. Photographs of MEHRRAFIEE near his vehicle and then MEHRRAFIEE inside his vehicle receiving a bag from Rajabi are shown below:



[13] Based on my review of California Department of Motor Vehicle records, I have learned that the SUBJECT VEHICLE has the VIN W1K6X7KB3RA258152.

[14] As set forth below, Rajabi was later arrested for his role in a scheme to launder and transmit $150,000 in cash that were taken from a victim as part of an investment fraud scheme.

d. MEHRRAFIEE then went to an East West Bank branch in Encino, California. He took the bag into the bank branch and exited with only a piece of paper. MEHRRAFIEE got into his vehicle and proceeded to drive back to the building containing SUBJECT PREMISES-1.

43. Based on my review of records from East West Bank, I have learned that on or about September 24, 2024, MEHRRAFIEE deposited approximately $380,100 in cash into Bank Account-4, a bank account in the name of "Advva" with account number ending in 2866. Bank Account-4 was opened on or about April 21, 2021, and MEHRRAFIEE is listed as the sole authorized signer on the account. On the signature card for the Bank Account-4, MEHRRAFIEE's job title is listed as "Dentist," and MEHRRAFIEE's phone number is listed as the MEHRRAFIEE Phone Number. The business address listed for Advva is SUBJECT PREMISES-1.

44. Based on my training and experience and knowledge of the investigation, I believe the sequence above reflects Rajabi handing MEHRRAFIEE a plastic bag containing currency, which MEHRRAFIEE then brought into the bank branch and deposited into Bank Account-4. Based on my training and experience, I believe this activity is consistent with unlawful money laundering and bulk money transmitting, rather than legitimate business activity.

3. This Week, Rajabi Was Charged and Arrested for Laundering Money in a Fraud Scheme

45. Based on my review of court records, I have learned that on or about February 6, 2025, Rajabi was charged in a

criminal complaint with violations of 18 U.S.C. § 1349 (conspiracy to commit fraud) and 18 U.S.C. § 1956(h) (conspiracy to commit money laundering). *See* No. 25-cr-20020-SHL (W.D. Ten.).

46. Based on my review of the Complaint against Rajabi, I have learned the following:

a. In April 2024, an individual in Germantown, Tennessee (the "Victim") was invited to invest in a cryptocurrency scheme and ultimately paid approximately $1,700,000 into a platform called CoinMetro. The Victim paid this money in wire transfers and in cash that was picked up in-person by conspirators.

b. Later in 2024 and into 2025, the Victim was told that if he/she wanted to make a withdrawal from his/her account, he/she would first have to pay tax. The Victim made several wire transfers to this end but was told he/she still owed tax. The Victim then reported the scheme to law enforcement.

c. In January 2025, the Victim told conspirators that he/she had $150,000 cash to deposit. Conspirators indicated they would send a courier to his/her house.

d. On February 3, 2025, a courier arrived in front of a home owned by the Victim as scheduled. The courier presented a previously-provided password and took the money. Law enforcement officers were surveilling the exchange and arrested a particular individual ("CC-5") with the money after he drove away.

e. CC-5 cooperated with law enforcement and admitted he was sent by a person he knew as Amir Hafezi ("HAFEZI") in Toronto, Canada. CC-5 admitted he was directed by HAFEZI to pick up the money in Memphis and drive it to a person named Mike in Los Angeles for handoff. CC-5 also admitted that moments before he was arrested by Tennessee law enforcement, he notified HAFEZI that he had picked up the money.

f. On February 4, 2025, CC-5, now acting at the direction of law enforcement, received from HAFEZI the contact name "Mike," later identified as Rajabi, and Mike's phone number, which ended in 8337 (the "Rajabi Phone Number"). Mike and CC-5 had several communications over the next two days wherein Mike set the meeting location and time at a Starbucks coffee shop in Woodland Hills, California, at 10:00 AM PST on February 6, 2025. Mike described the car he would be driving and indicated they should meet at the corner of the parking lot.

g. On February 6, 2025, Mike then appeared at the agreed-upon location, at approximately the agreed-upon date and time, and in a vehicle that matched the description Mike previously gave to CC-5. Mike went to the corner of the parking lot and exchanged text messages with CC-5 indicating that he (Mike) had arrived for the meeting. Agents then approached and arrested the individual, who was identified as Rajabi. Agents recovered the two cellphones from on top of the center console area of the Rajabi's vehicle.

47. On or about February 6, 2025, the Hon. Alicia G. Rosenberg, United States Magistrate Judge, authorized warrants

to seize and search two cellphones inside Rajabi's vehicle as well as the vehicle itself. *See* Case Nos. 2:25-mj-541, 542. Based on my preliminary review of one of the cellphones seized from Rajabi's vehicle, I have learned the following:

a. Between approximately July 17, 2023, and February 4, 2025, MEHRRAFIEE and Rajabi exchanged messages via WhatsApp. Rajabi frequently sent photographs of bank deposit receipts to Mehrrafiee. On or about September 16, 2024, Rajabi sent a photograph of a Bank of America deposit receipt indicating a check was deposited for approximately $47,000. The messages include photos of a driver's license belonging to neither MEHRRAFIEE nor Rajabi, and the address for a Bank of America account.[15]

b. Both MEHRRAFIEE and Rajabi exchanged photographs showing cryptocurrency transactions and wallets. On or about October 24, 2024, MEHRRAFIEE sent a cryptocurrency wallet to receive money to Rajabi. Rajabi responded sending a screenshot indicating a transaction was completed using the cryptocurrency "USDT" to the wallet that MEHRRAFIEE sent. Rajabi sent an additional screenshot indicating approximately 289,900 USDT was being sent to the same wallet. On or about October 28, 2024, this same pattern occurred again. Rajabi sent a screenshot indicating 399,900 USDT was sent to the same crypto wallet. The screenshot indicated that this was the equivalent of approximately $399,698.

[15] The exchanges between MEHRRAFIEE and Rajabi contained many foreign-language messages, which have not yet been translated.

c. On or about February 21, 2024, MEHRRAFIEE sent a text message to Rajabi telling Rajabi to come to the Balboa office, *i.e.*, SUBJECT PREMISES-1.[16] On or about October 16, 2024, Rajabi sent a text referencing the building containing SUBJECT PREMISES-1, this time asking if that was the correct address.

d. On or about May 17, 2024, Rajabi sent a message to MEHRRAFIEE stating "212,260 cash, 36,740 money order, total is 249,000."

48. On or about January 14, 2025, the Hon. Alka Sagar, United States Magistrate Judge, authorized the installation of pen registers and trap-and-trace devices to record incoming and outgoing communications via WhatsApp and T-Mobile for the MEHRRAFIEE Phone Number. *See* Case Nos. 2:24-mj-107, -108.

49. Based on my review of pen register and trap-and-trace records, I have learned that between January 27, 2025, and February 4, 2025, there were approximately 14 WhatsApp communications between the MEHRRAFIEE Phone Number and the Rajabi Phone Number. As described above, Rajabi messaged with co-conspirators in his fraud and money laundering offense leading up to his arrest on February 6, 2025.

50. On or about February 7, 2025 – the day after Rajabi's arrest – I learned that MEHRRAFIEE has travel booked on February 9, 2025, to go from Los Angeles International Airport to Dubai, United Arab Emirates, and then from Dubai to Tehran, Iran. Based

[16] The content of this message was in a foreign language, which I translated using a publicly available translating service.

on my review of immigration records, MEHRRAFIEE is an Iranian citizen and a lawful permanent resident in the United States.

4. Bank Records and Surveillance Show MEHRRAFIEE Conducting Similar Meetings and Deposits

51. Based on my review of FBI surveillance reports, I have learned the following:

a. On or about September 23, 2024, FBI Special Agents conducting surveillance saw MEHRRAFIEE exiting the building containing SUBJECT PREMISES-1. As set forth above, the address for SUBJECT PREMISES-1 is also the business address listed for Advva in California Secretary of State business records.

b. During surveillance on September 23, 2024, Special Agents saw MEHRRAFIEE carrying a plastic shopping bag. MEHRRAFIEE went to the same East West bank branch in Encino, California, that would visit again the next day, as described above. MEHRRAFIEE carried the bag into the bank. Upon exiting the bank, MEHRRAFIEE did not have the bag and was carrying a small sheet of paper.

52. Based on my review of East West Bank records, I have learned that on or about September 23, 2024, MEHRRAFIEE deposited approximately $580,000 in cash into a bank account at East West Bank in the name of "I Concert Entertainment LLC" with account number ending in 6511 ("Bank Account-6"). Bank records show frequent large cash deposits into Bank Account-6. For example, on or about August 5, 2024, there was a deposit of $599,800 in cash. Three days later, on or about August 8, 2024,

there was a deposit of $1,050,000 in cash. One week later, on or about August 15, 2024, there was a deposit of $337,900 in cash.

53. Based on my review of FBI surveillance reports, I have learned the following:

a. On or about October 28, 2024, FBI Special Agents doing surveillance saw MEHRRAFIEE park in a strip mall parking lot. An individual ("CC-6") entered the passenger side of MEHRRAFIEE's car. The two of them then exited MEHRRAFIEE's car and walked over to CC-6's car. There, they opened the trunk and MEHRRAFIEE took a small box from the trunk. MEHRRAFIEE returned to his vehicle alone with the box. MEHRRAFIEE then drove to a JPMorgan Chase bank branch and parked outside the bank. Agents doing surveillance then saw MEHRRAFIEE interact with the driving in Vehicle-1, *i.e.*, the vehicle driven by Rajabi on September 24, 2024; however, agents doing surveillance did not identify the driver of the vehicle in their report. MEHRRAFIEE left the bank and traveled to the building containing SUBJECT PREMISES-1.

b. On or about November 12, 2024, and November 25, 2024, FBI Special Agents saw MEHRRAFIEE depart his residence (*i.e.*, SUBJECT PREMISES-2) and drive to the same BMO Bank branch. On both dates, after leaving the bank, MEHRRAFIEE went to SUBJECT PREMISES-1.

I. MEHRRAFIEE's Purported Business is at SUBJECT PREMISES-1 and He Frequently Visits the Premises

54. As set forth above, MEHRAFFIEE's Advva bank account statements list SUBJECT PREMISES-1 as the business address. On September 24, 2024, agents saw MEHRRAFIEE travel from SUBJECT

PREMISES-2 to meet with Rajabi, deposit approximately $380,000, then travel to the building containing SUBJECT PREMISES-1. The day before, September 23, 2024, agents also saw MEHRRAFIEE leaving the building containing SUBJECT PREMISES-1 and he deposited $580,000 the same day into Bank Account-6. On February 24, 2024, MEHRRAFIEE told Rajabi come to come to SUBJECT PREMISES-1.

55. Based on surveillance and publicly available information, I know that SUBJECT PREMISES-1 is associated with the business "Advva," which purports to conduct advertising and marketing work. Based on my review of a LinkedIn page for MEHRRAFIEE, he is the "Founder and CEO" of Advva. On February 9, 2025, I attempted to access the website associated with Advva (www.advva.com), and the internet search returned a screen stating, "Service Unavailable." Using the internet archiving service, Waybackmachine, I reviewed historic internet pages associated with www.Advva.com and saw website features related to a business offering advertising services. Among other things, I saw the following related to Advva: "My name is Shirzad, and I'm the founder and CEO of Advva. We've revolutionized advertising with our patented mobile billboard technology that puts your brand on the map—literally. Our moving ads capture attention in ways stationary billboards and digital ads simply can't match."

56. Furthermore, as set forth above, MEHRRAFIEE's purported businesses, although not Advva, received hundreds of thousands of dollars from the 17 Alias Bank Accounts. *See*

Paragraph 19.c, *supra*. I am not aware of any connection between the aliases that were used to submit fraudulent EIDL applications and the purported business that MEHRRAFIEE operates. Based on my training and experience, this demonstrates that MEHRRAFIEE combines his fraud schemes with his business activity and does not keep those activities separate.

57. Based on my review of California Franchise Tax Board records and bank records, I have learned the following:

a. Advva reported little business activity to the California Franchise Tax Board for the years 2020-2023. Specifically:

i. For 2020, the business reported no income on its S Corporation Franchise or Income Tax Return and stated that it began in California or first derived income in California on December 21, 2020.

ii. For 2021, the business reported no income on its S Corporation Franchise or Income Tax Return and paid $800 in tax to the California Franchise Tax Board. In an appended copy of the business's federal Form 1120-S, Advva again reported no income and no shareholders other than MEHRRAFIEE.

iii. For 2022, the business reported no income on its S Corporation Franchise or Income Tax Return and paid $800 in tax to the California Franchise Tax Board. The business stated that the beginning balance of its retained earnings was $162,327, it made no income, and its ending balance was the same amount.

iv. For 2023, the business reported no income on its S Corporation Franchise or Income Tax Return and paid $800 in tax to the California Franchise Tax Board. The business stated that the beginning balance of its retained earnings was $546,729, it made no income, and its ending balance was the same amount.[17]

v. Based on my training and experience, the California Franchise Tax Board filings show little business activity being conducted by Advva, MEHRRAFIEE's purported marketing business.

b. By contrast, bank records show that, between approximately March 2020 and October 2024, MEHRRAFIEE deposited approximately $15.9 million into the Advva bank account, Bank Account-4. MEHRRAFIEE transferred approximately $16.3 million from Bank Account-4 to other bank accounts MEHRRAFIEE controlled at East West Bank.[18]

c. Based on my training and experience, this significant difference between reported business activity and

---

[17] I have not received a copy of Advva's filings with the California Franchise Tax Board for tax year 2024.

[18] Based on my review of bank records, I have also learned that MEHRRAFIEE transferred approximately $3.1 million from Bank Account-4 to businesses that deposited or cashed checks at Hermanos 3 Mercado, which is a check cashing business.

Records provided by East West Bank for Bank Account-4 also include California Secretary of State filings for Advva. Based on my review of those filings, I know that in Advva's corporate filings, Advva listed a business address at 17530 Ventura Blvd., Suite 203, Encino, California 91316. Advva also listed the same address on its California Franchise Tax Board filings, as described below. However, as set forth above, a placard outside the entryway to SUBJECT PREMISES-1 also lists "Advva" and agents have seen MEHRRAFIEE traveling to and from SUBJECT PREMISES-1, as described herein.

bank account activity is unusual and consistent with MEHRRAFIEE's suspected money laundering and unlicensed money transmitting schemes, described above, rather than legitimate business activity by Advva.

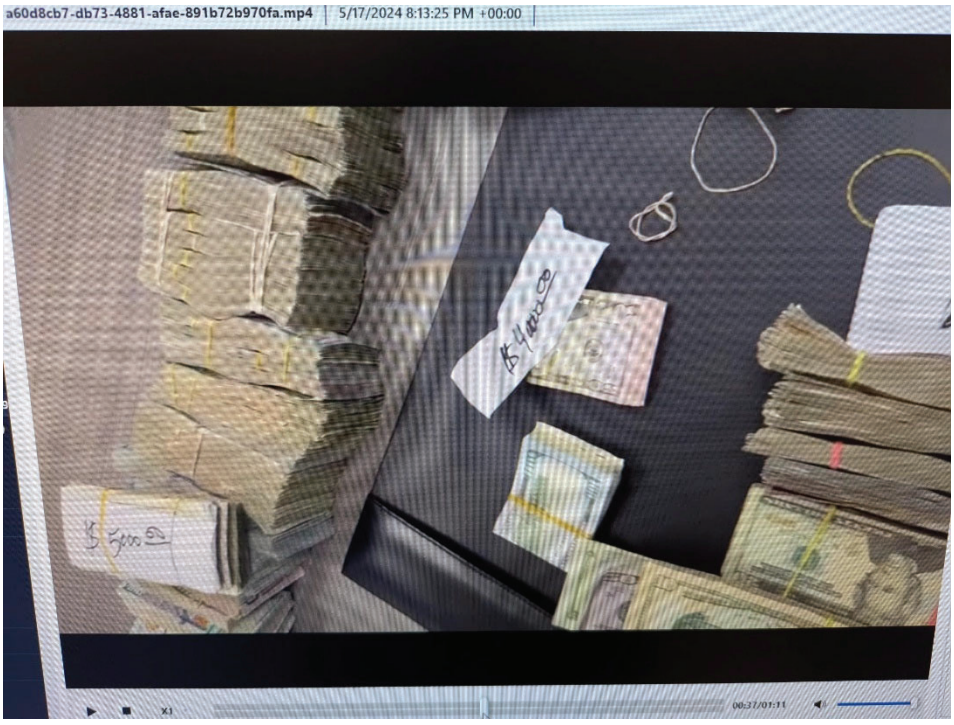
58. Based on my review of records from the MEHRRAFIEE iCloud Account pursuant a search warrant, I have learned the following:

a. MEHRRAFIEE iCloud Account records include a photograph of a bulk quantity of United States currency that was taken from inside SUBJECT PREMISES-1. I have identified the location as SUBJECT PREMISES-1 based on another photograph in the MEHRRAFIEE iCloud Account, which shows MEHRRAFIEE in an Advva office with the same distinctive carpet that is shown in the photograph with the United States currency. The two photographs are shown below:

Photograph showing bulk United States Currency

Photograph from inside Advva office, with MEHRRAFIEE in the middle

b. On or about May 17, 2024, MEHRRAFIEE sent a video via WhatsApp to Rajabi. The video appears to show the Advva office, which has approximately six small offices surrounding a common space. The video shows one individual at a desk in the office, another individual inside the business, and MEHRRAFIEE. The office is sparsely decorated. In the video, MEHRRAFIEE shows the camera multiple rubber-banded stacks of currency and checks. The cash appears to be placed on a desk that is consistent with previous photos of MEHRRAFIEE's desk at SUBJECT PREMISES-1. In the photo, some of the written placards display $100,000, $40,000, $20,000 5,000 and more that are not visible. There appear to be approximately 21 rubber banded stacks of cash, checks, and money grams. The photograph below comes from the video recorded by MEHRRAFIEE and sent to Rajabi:



59. On or about January 30, 2025, the Hon. Stephanie S. Christensen, United States Magistrate Judge, authorized a warrant for historical and prospective location data for the cellphone associated with the MEHRRAFIEE Phone Number (the "Location Data Warrant"). Based on my review of prospective location data obtained pursuant to this warrant, I have learned that MEHRRAFIEE's phone is frequently located in the vicinity of SUBJECT PREMISES-1, including as recently as February 7, 2025.

60. Based on my training and experience, given the large quantities of cash and currency transmitted by MEHRRAFIEE, I believe records of the Subject Offenses may be found in SUBJECT PREMISES-1. The records particular to SUBJECT PREMISES-1 may include ledgers of cash transactions, deposit slips, currency packaging and counting machines, records discussing sources and destinations of funds, and digital devices that may contain evidence of the Subject Offenses, as described below.

J. MEHRRAFIEE Lives At SUBJECT PREMISES-2

61. As set forth above, on or about June 23, 2021, MEHRRAFIEE applied for and received a mortgage on the property located at SUBJECT PREMISES-2.

62. Based on my review of records from the MEHRRAFIEE Email Accounts obtained pursuant to a search warrant, I have learned the following:

a. MEHRRAFIEE receives daily emails from the United States Postal Service with a preview of the mail to be received that day at SUBJECT PREMISES-2. These emails show, among other things, that MEHRRAFIEE frequently receives financial records at

SUBJECT PREMISES-2. Furthermore, MEHRRAFIEE has received mail from Luxury Watch as recently as January 2, 2024. As set forth above, Luxury Watch received a significant sum of money disbursed as a result of the 17 Alias EIDL Applications. The mail reflected in these United States Postal Service emails were directed to SUBJECT PREMISES-2 and their contents may be obtained by searching the premises.

b. United States Postal Service emails also show that on or about October 28, 2024, BMO Bank sent to SUBJECT PREMISES-2 what appeared to be statements to for American Golden Brokers and I Concert Entertainment. On or about February 20, 2024, Ally Bank sent to SUBJECT PREMISES-2 a bank statement to I Concert Entertainment.

63. On or about December 18, 2024, FBI Special Agents conducting surveillance, saw MEHRRAFIEE depart the vicinity of SUBJECT PREMISES-2. As set forth above, on September 24, 2024, MEHRRAFIEE left SUBJECT PREMISES-2 to meet with Rajabi. On or about October 25, 2024, MEHRRAFIEE was seen departing in the SUBJECT VEHICLE in vicinity of SUBJECT PREMISES-2. MEHRRAFIEE made one stop and went to BMO Bank in Encino, California. MEHRAFFIEE departed BMO bank and proceeded to SUBJECT PREMISES-1.

64. Based on my training and experience, I know that individuals involved in fraud offenses may keep relevant evidence and fruits in their businesses and in their homes. Homes are particularly likely to have older digital devices that may still have relevant records; ledgers of unlawful activity

kept in a security area away from employees; and evidence of otherwise innocent activity – like travel or luxury purchases – that are actually evidence of the Subject Offenses by showing the location of co-conspirators and the spending of fraud proceeds. For the reasons set forth a below, digital devices kept in the home, like an Apple iPad or laptop computer, may be synchronized with cellphone devices and cloud storage platforms to contain key electronic communications in furtherance of the Subject Offenses. Moreover, in the post-COVID-19 work landscape, many individuals have fully-functioning home offices that mirror or synchronize the records kept in a business office like SUBJECT PREMISES-1.

65. Based on my review of prospective cellphone location data obtained pursuant to the Location Data Warrant, I have learned that MEHRRAFIEE's phone is frequently located in the vicinity of SUBJECT PREMISES-2, including as recently as February 8, 2025.

* * *

66. As set forth in Attachment B, I am seeking records for the period from January 1, 2019, to February 9, 2025. Records beginning on January 1, 2019, are relevant because that was the approximate beginning of the time period for which MEHRRAFIEE had to make representations on EIDL applications. Moreover, for all Subject Offenses, records beginning at this time may show connections between co-conspirators and show plan and preparation. The schemes described above are sophisticated criminal operations that require many co-conspirators, trust

among co-conspirators, expertise in evading law enforcement, and navigation of banking rules and regulations. The amount of money being laundered by MEHRRAFIEE also strongly suggests that he has laundered proceeds before and that co-conspirators trust him with significant quantities of money. Records through the date of the proposed warrants may be relevant to show reactions to the success or failure of the scheme, efforts to continue laundering funds, efforts to conceal the subject offenses, conduct towards additional victims, plan and preparation for the criminal transactions culminating in Rajabi's arrest on February 6, 2025, reactions to Rajabi's arrest that would show consciousness of guilty and involvement in the same scheme, and evidence of MEHRRAFIEE's flight from prosecution.

K. Training And Experience Regarding The Subject Offenses And Electronic Evidence

67. Based on my training, experience, and knowledge of the investigation, I am aware of the following regarding fraud, money laundering, and money transmitting schemes like the ones operated by MEHRRAFIEE:

a. Individuals involved in the Subject Offenses often collect checks, access devices, other personal identifying information (such as names, Social Security numbers, and dates of birth), and identification documents belonging to other people that they can use to fraudulently obtain money and items of value. It is a common practice for those involved in such crimes to use either false identification or stolen real identification (like the aliases underlying the 17 Alias EIDL

Applications) to make purchases with stolen access devices at in order to avoid detection and to complete the transaction. Those who engage in such fraud keep evidence of such fraudulent transactions.

b. It is common for individuals engaged in the Subject Offenses to use equipment and software to print identification cards (like the "plastic IDs" referenced above), to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. Software relevant to such schemes can often be found on digital devices, such as computers and cellular telephones. Such equipment and software are often found in the thieves' possession as they can be small and easily portable.

c. It is common practice for persons involved in the Subject Offenses to possess and use multiple digital devices at once, like the two cellphones Rajabi was carrying at the time of his arrest. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and false aliase. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts

and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential fraud and identity theft victims; (6) verifying the status of stolen access devices; and (7) coordinating with co-conspirators. Given the seamless transition between co-conspirators, MEHRRAFIEE's contact with multiple individuals, and the particular sophistication of the scheme, I believe it is very likely that conspirators were each using one or more digital devise to further the scheme.

d. Individuals who participate in the Subject Offenses often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos.

e. Cash couriers are often employed in the Subject Offenses to minimize the ability to trace the proceeds. A courier will typically be directed by a "handler," who is someone else in the conspiracy who will orchestrate where to send the money.

f. Moving cash and handing it off to another member of the conspiracy to reintroduce the funds to the banking system or other form is a method of effectively laundering the proceeds

of a fraud scheme because it conceals the origins of the funds and obfuscates discovery of its eventual location.

g. Individuals engaged in the Subject Offenses, like those engaged in other complex criminal activity, frequently possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track transactions in furtherance of the scheme. Individuals involved in those crimes often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting transactions electronically and over the internet.

h. Information on digital devices is frequently backed up to online services, like Apple iCloud, Apple Drive, or Google backup service, and documents, communications, location data, and activity information from digital devices is frequently backed up to online services. Backup services can allow an individual to share data between multiple electronic devices, such as sharing contacts, settings, messages, and calendar information. In this case, RAJABI had multiple cellphones suggesting his use of multiple cellphones concurrently. The files may also be recoverable from a digital device even if they were manually deleted by the user.

68. Based on my training and experience, I know that individuals who engage in schemes like the ones conducted by MEHRRAFIEE frequently rely on cash proceeds from a number of different victims. Due to the cash nature of the business and the volume of victims and money pick-ups, individuals involved in these schemes frequently use their vehicles to travel to meet

with co-conspirators, victims, and third parties necessary for the success of the scheme. For example, as set forth above, MEHRRAFIEE met with Rajabi to collect money that he then deposited into a bank account. Because individuals engaged in these schemes transact in large quantities of cash, they often use different financial accounts and money laundering schemes to transfer and conceal their proceeds. That may involve driving to different banks and meeting with different co-conspirators. To conceal their scheme, they also frequently meet in person with victims to retrieve money, rather than using digital transfers that would be more easily traceable. Records of the scheme to defraud itself (like handwritten addresses of victims and false identity documents), movement of the proceeds (like bank statements), movement of co-conspirators (like travel records) and money laundering (like digital devices used to talk about hiding transfers) may be found in the vehicles that are used as part of this fraud, like the SUBJECT VEHICLE.

L. Training And Experience Regarding Digital Devices

69. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the

hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading

filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

70. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

71. The search warrant requests authorization to use the biometric unlock features of a device, based on the following,

which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Shirzad MEHRRAFIEE's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of

MEHRRAFIEE's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

V. CONCLUSION

72. For all of the reasons described above, I submit that there is probable cause to believe that MEHRRAFIEE committed a violation of 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud).

73. Furthermore, I submit that there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found in SUBJECT PREMISES-1, SUBJECT PREMISES-2, and the SUBEJCT VEHICLE and on MEHRRAFIEE's person, as described in Attachments A-1, A-2, A-3, and A-4.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 9th day of February, 2025.

Alicia G. Rosenberg

THE HON. ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The property to be searched is 6345 Balboa Boulevard, Building 3, #257, Encino, California 91316 ("SUBJECT PREMISES-1"). SUBJECT PREMISES-1 is contained within a three-story commercial office building with a white exterior and the words "ENCINO OFFICE PARK III" over one entrance. SUBJECT PREMISES-1 is on the second floor of the building.

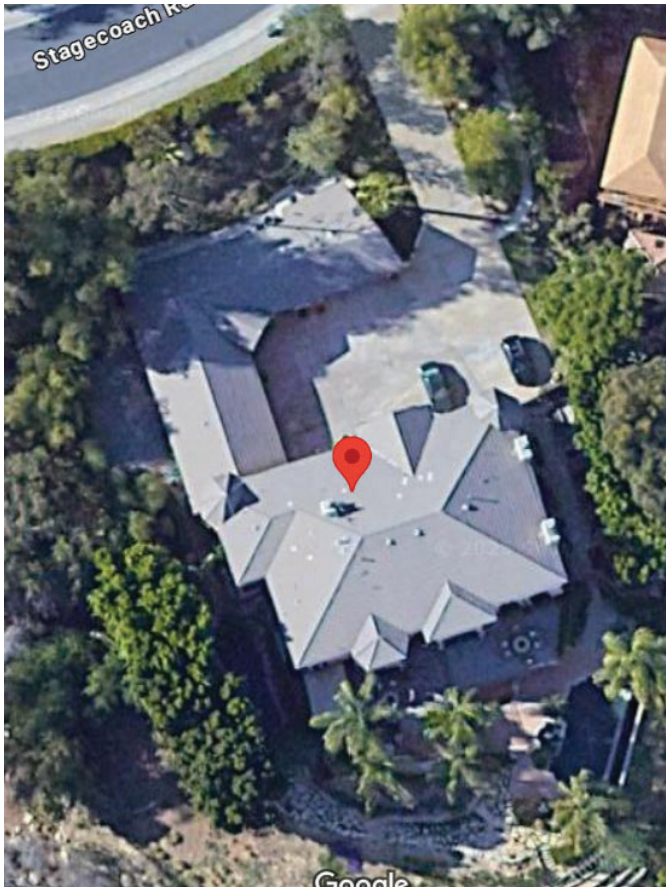
There is a small sign to the left of the door to SUBJECT PREMISES-1. The sign reads "257" and "Advva." The door to SUBJECT PREMISES-1 is white and is shown below:

ATTACHMENT A-2

PROPERTY TO BE SEARCHED

The property to be searched is located at 84 Stagecoach Road, Bell Canyon, California 91307 ("SUBJECT PREMISES-2"). SUBJECT PREMISSES-2 is an approximately 12,124 square foot single family residence on a 1.44 acre lot. The exterior is a beige stucco material and a tile roof. The building is three-stories with a pool, pond, and four-car garage.

SUBJECT PREMISES-2 is shown below:



ATTACHMENT A-3

PROPERTY TO BE SEARCHED

The property to be searched is the white Mercedes Maybach, California license plate 9LCT781 and Vehicle Identification Number ("VIN") W1K6X7KB3RA258152.

ATTACHMENT A-4

PROPERTY TO BE SEARCHED

The person to be searched is the person of Shirzad MEHRRAFIEE, whose date of birth is May 6, 1980. MEHRRAFIEE is approximately 5'11" tall and weighs approximately 210 pounds.

The search of MEHRRAFIEE shall include any and all clothing and personal belongings, digital devices, backpacks, luggage, wallets, briefcases, purses, folders, bags, and other containers carried or held by the person, or that are within MEHRRAFIEE's immediate vicinity and control at the location where the search is executed.

MEHRRAFIEE's face is shown below:

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud); 18 U.S.C. § 1956 (Money Laundering); 18 U.S.C. § 1957 (Transacting in Criminal Proceeds Over $10,000); 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering); 18 U.S.C. § 1960 (Unlicensed Money Transmitting Business); 15 U.S.C. § 645 (False Statements to the SBA); and 18 U.S.C. § 371 (Conspiracy to Make False Statements to the SBA) (the "Subject Offenses"), from January 1, 2019, to February 9, 2025, namely:

a. Records regarding the ownership or operation of any business associated with Shirzad MEHRRAFIEE, including any of the following businesses or their affiliates: I Concert Entertainment, Platinum Entertainment Group, Exotic Secrets LLC, Shirzad Music, American Golden Coverage Brokers, LAA Group, Platinum Entertainment Group, Café Taraneh, Atila Investments, Lux Dental Spa, Wilshire Center Insurance Services, or Road Ad;

b. Records regarding the possession or use of any aliases other than Mehrrafiee, including any identifying information belonging to others, the use of any other aliases to apply for Paycheck Protection Program or Economic Injury Disaster Loan ("EIDL") loans, or the use of any other aliases to open bank accounts or launder proceeds;

c. Records regarding any actual or attempted claim

for COVID-19 benefits, including records regarding the success or failure of such claims and the proceeds of such claims;

d. Records regarding the receipt or transmission of photographs or video in furtherance of the Subject Offenses, including common money laundering techniques like the transmission of codes or serial numbers;

e. Records regarding representations about cryptocurrency investments or investment in a cryptocurrency business;

f. Records regarding efforts to send, receive, store, or transfer bulk quantities of currency or cryptocurrency;

g. Records regarding efforts to send, receive, store, or transfer with concealed methods, like false or stolen aliases, structured transfers lower than $10,000, or by means that bypass banks like cash transfers;

h. United States currency in excess of $1,000, including the first $1,000 if more than $1,000 is found;

i. Any and all cryptocurrency, to include the following:

i. Any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;

ii. Any and all representations of cryptocurrency private keys, whether in electronic or physical format;

iii. Any and all representations of

cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "recovery seeds" or "root keys," which may be used to regenerate a wallet; and

iv. The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States;

j. Records relevant to preparatory steps in furtherance of the Subject Offenses, such as communications with co-conspirators regarding the receipt of funds, meeting locations, and banking information;

k. Records regarding efforts to conceal the Subject Offenses or avoid detection by law enforcement;

l. Records relevant to and showing communication with co-conspirators in the Subject Offenses;

m. Records related to the nature and development of the relationships among co-conspirators in the Subject Offenses;

n. Records related to motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations;

o. Records regarding financial transactions in furtherance of the Subject Offenses and records regarding banking and online accounts used by a conspirator in the Subject Offenses;

p. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof; and

q. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device; and

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. **SEARCH PROCEDURE FOR DIGITAL DEVICES**

4. In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

c. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

d. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

e. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

f. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

g. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

h. If the search determines that a digital device does contain data falling within the list of items to be seized,

the government may make and retain copies of such data and may access such data at any time.

i. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

j. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

k. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the

government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress Shirzad MEHRRAFIEE's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of MEHRRAFIEE's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.